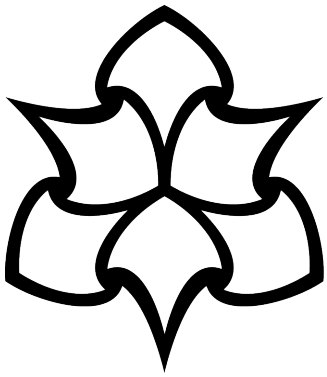


Do Europe's borders need multi-faceted biometric protection?


Keeley Crockett


James O'Shea


Lukasz Slarski


Anna Malamou


Georgios Boultadakis

Keeley Crockett and James O'Shea, Manchester Metropolitan University. Székely Zoltán, Hungarian National Police. Tukasz Szklarski, iTTi. Anna Malamou and Georgios Boultadakis, European Dynamics

In today's world, terrorism has become a dire and global threat. Within Europe, terror attacks and participation in terrorist organisations by EU citizens are on the rise. To deal with this, the European Union has introduced some significant legal changes to the Schengen agreement – the treaty that led to the creation of Europe's Schengen area where internal border checks have largely been abolished. The most recent and interesting of these changes has meant that systematic controls are being introduced at border crossings.

"Solutions identified include the pre-arrival registration and biometric identification of people to speed up the process, and wearable intelligent border control equipment"

In effect, from 7 April, a new EU rule (Regulation 2017/458) has reinforced checks against relevant databases at external borders. This makes checking EU citizens and their travel documents against databases compulsory, enhanced with biometric checks where needed. It means that at the border gates, instead of checking EU citizens randomly, they should all be checked. Until now, only third-country citizens came under such a rule, so the new regime will have a very strong impact on the dynamics of Europe's cross-border traffic.

Consider the numbers in Hungary, as an example. Currently, third-country citizens represent around 22% of the total crossings at Hungarian borders, while 78% are Hungarian nationals or other EU citizens and persons enjoying the right to free movement. In 2015, of the 42.2m people crossing Hungary's external borders, 9.3m were checked because they were third-country citizens and about 3m were checked on a random basis out of all the EU citizens. But as from April 2017, all 32.9m EU citizens have to be checked.

Of course, biometric data can potentially contribute to a faster, more secure and feasible verification of people's identity. In light of this, the ongoing Horizon 2020 'Intelligent Portable Control System' project has been established, in tandem with a number of European border authorities. The project's aim has been firstly to identify any problems in the daily routines of the EU border control system, and then propose how technology could be developed to help those involved carry out their duties in a more effective and less risky manner.

The solutions identified by the project include the pre-arrival registration and the biometric identification of people to speed up the process[1] and wearable intelligent border control equipment that will allow the capacity for control to be enlarged, even where the infrastructure cannot be physically extended (such as at a railway border crossing point) by increasing the headcount of the border control force.

Without such innovative technology, a traveller could easily face the same queues and waiting times as in the 1980s and 1990s[2], resulting in the benefits of a dynamic cross-border flow being lost. This is the core advantage of the Schengen regime, and slowing the

Requirements extraction

Collecting the requirements for the Intelligent Portable Control System required an in-depth knowledge and analysis of the border point crossing function, from the user perspective. The requirements methodology used multiple techniques with their own specific values, in order to gain a complete picture. In the case of this project, assuming that a representative sample of border guards and border managers could be available for face-to-face interaction, a series of site-surveys, workshops, questionnaires and structured physical interviews were carried out.

More specifically, site surveys and workshops have been helpful for gathering information on current processes. This opportunity for observation overcame the difficulty that some people face in explaining what they do and why, especially when their work routine has become habitual. The opportunity to monitor how the officers actually perform their job helps to achieve a better understanding of the entire picture, and to experience the work and the different tasks/routines of the users.

For this reason, a visit to the Tompa-Kelebia border crossing point, organised by the Hungarian Police, provided a unique opportunity to observe how the procedures are implemented in a real situation and provided a better understanding of how new technologies can fit in these procedures. What's more, face-to-face contact with users through individual interviews was used as the primary source of requirements, and an important way to gather and validate the requirements.

For this reason, in-depth, semi-structured interviews and questionnaires were designed and carried out with a representative sample of employees. The aim of the interviews was to identify any problems they faced in performing their daily routines and to explore how the proposed new system could help them. Interviews were carried out with both border guard managers and with officers such as passport control officers and document/vehicle experts based on their position, experience and working conditions at the border crossing points in Hungary, Greece and Latvia.

The categorical answers from the interviews were analysed using elementary data analysis techniques[5].

border crossing process could result in a direct cut in the average 2.3% GDP increase created by Schengen[3]. Solutions like the ones proposed by the project could keep waiting times at low levels, while providing the increased security the EU is looking for, all at the same time. Moreover, the project could open a path to the next generation enhancement of the EU's integrated border management system[4].

Market opportunity: research outcomes

The Intelligent Portable Control System project has led to a series of findings about the best application of different biometric modalities in border control. But the core basis for these recommendations has been careful research (see 'Requirements extraction' box). In effect, the decisions taken about whether and how to implement biometric solutions in the project were driven by the results of direct interviews with border guard agents. Their answers revealed the end user requirements that must be taken into account during the project's implementation process. So what, from an insider's perspective, are the main preferences regarding the use of biometrics in the border control process? And what are the challenges and new opportunities that the project should consider? The key findings can be summarised as follows:

• Palm vein scanner technology was deemed to be a very reliable and easy way of obtaining unique patterns for identification and was recognised as being far more secure than fingerprints. The data obtained during palm vein scanning is impossible to counterfeit and, as a result, such scanners provide an optimal environment for fast and secure biometric authentication. However, one comment worth mentioning raised the issue of susceptibility to dirt (the cleanliness of hands) as a potential technical problem. The majority of the responses, though, underlined the innovative nature of palm vein scanner technology and proposed that the system should support palm vein scanners as the main tool for establishing travellers' identities.

• Most respondents strongly emphasised the usefulness of facial recognition technology. The most commonly repeated argument was that this technology could support the work of border guard agents, who are not able to capture all the details of a face in order to identify travellers sufficiently. Some agents were unsure about the effectiveness of this technology in dealing with intentional or unintentional changes to the image of a traveller's face (ie, beard, moustache, scars, glasses). The concern was this could lead to a possible distortion and inability to easily identify the person's identity. A few responses also highlighted a potential mismatch between face recognition and the facial photo in the passport. These views rather emphasised that facial recognition technology is complementary to any proposed new solution and highlighted the need to connect face recognition with data drawn from other biometric solutions.

Palm vein scanner detection through the illumination of blood vessels via infrared light. ***Image credit: BIOSEC***

• Fingerprint technology was confirmed by the majority of border guards as a proven way to check the validity of a traveller's visa. They also indicated a strong level of commitment and confidence in this biometric data identification technique. However it was noted that fingerprint systems require complicated procedures and large amounts of data to be processed. As a result, this technology was seen as only partially suitable and there were strong recommendations that it should be replaced either by new-generation technology or by palm vein scanning. Some respondents also revealed that current fingerprint readers face problems in cold weather, due to the change in travellers' skin characteristics.

Survey results

All the respondents agreed that the application of biometric palm vein scanning, face recognition and fingerprinting technology could improve the speed of traveller checks at the border. Given that the survey questioned border guard officers across different countries, representing people of varying work experience, the conclusions drawn from this research – and the end user requirements consequently drawn up by this project – are of major importance. All the interviewees emphasised the need for new solutions that include biometric technologies, to enable border traffic flow to be improved. It should be noted that most border managers and officers were eager to adopt new biometric technologies and believed that in this way they could improve their working conditions, shift management and resources allocation.

The border guards' recommendations have paved the way for the further development of the project, where biometrics will play a major role in fulfilling end users' expectations. The project will incorporate biometric technologies, both in the pre-registration phase (where the traveller goes through an automated initial check and interview before their arrival at a border) and at the border crossing point. In order to address the issues outlined above, the system architecture is currently being designed to include palm vein scanners as the main identification tool. Face recognition will be used as a complementary tool, and fingerprints devices already in place at the border control points will be used in order to remain in line with the existing regulatory framework.

"Most border guards proposed that the system should support palm vein scanners as the main tool for establishing travellers' identities"

The main goal of this project is to promote biometrics as a mainstream method for traveller identification. And in terms of market take-up, the use of new biometric technologies at EU border crossing checks is likely to be adopted worldwide, due to a number of benefits. These include increased security, reduced check-in times of travellers (both the entry and exit time at the border crossings, and the clearance time of individual travellers), better management of the flow of traffic, and increased efficiency and accuracy in travellers' border checks.

Implementation issues

The project has also explored the issues around introducing these innovations. The implementation process is complex, encompassing not only novel biometric solutions but also related biometric analytics, detection and communication tools. Of course, the use of current biometric solutions is part and parcel of contemporary border management, which needs to provide enhanced security as well as improved cross-border movement. Border authorities and officers put a premium on both these factors. Consequently, and based on the results of the end user requirements collection, the project assumes the implementation of a face-matching

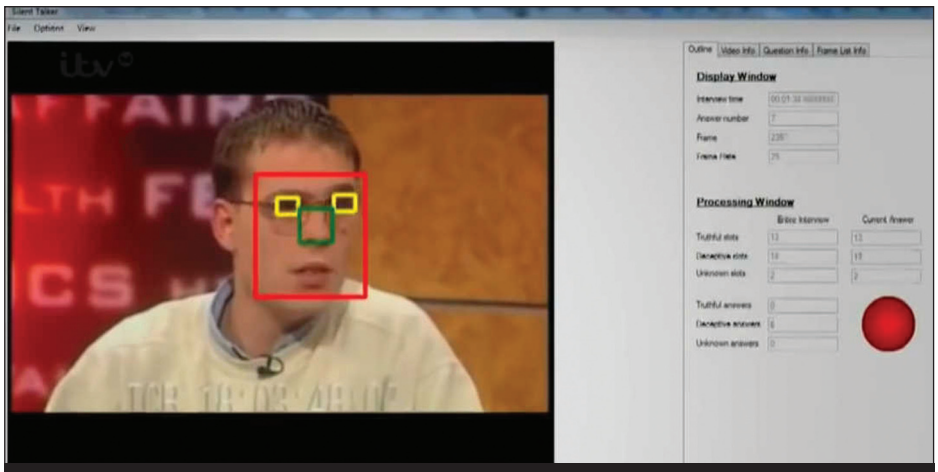
tool, palm vein scanner, fingerprint recognition and an automatic deception detection system.

Face recognition is a relatively well-grounded biometric solution characterised by high public acceptance – which was confirmed in the process of eliciting user requirements. The developed face-matching tool will operate at two stages of cross border procedures – pre-arrival registration and border crossing. The first verification will be done remotely, offline. The system will retrieve the image of the traveller captured during their interaction with the automatic deception detection system and will compare it with the uploaded passport photograph. The latter verification, at the border, will rely on capturing a live, high resolution image of the traveller at a border crossing point and comparing it with the person's electronic image (in the case of e-passports) or passport photo. The system will then run a final verification, where the results of the pre-arrival phase are compared with the border check results, in order to determine whether it is the same person.

The face-matching tool implemented within the project is designed to overcome frequently associated problems with face recognition. For instance, the tool will consider the differences in image quality between the scanned and original photograph, which is possible due to the extraction of invariant facial features including shapes, local patterns and biological features. The use of global features (shapes, geometrical data) as well as local features (facial characteristics) is intended to further enhance the verification process. The face verification process will also make allowances for natural variations in lighting, aging, facial marks and expression. In addition, the tool will be versatile in its application, since it will be dedicated to a traveller's device (laptop, mobile phone etc), which will be used in the pre-arrival phase; and it will co-operate with the body-mounted camera used at the human agent interview at the border crossing point.

Besides the face-matching tool, the project also incorporates fingerprint and palm vein recognition technology in a secure mobile unit used by border officers. The aim is to equip guards with tools that enable them to perform more robust verification and speed up the decision-making process. The use of fingerprint recognition for verification is already a well-known security measure in border procedures, as travellers have their fingerprint's pattern incorporated on an e-passport's chip. However, the security level of commercially available solutions is relatively low. Therefore, the application of a single modality fingerprint sensor might be risky, especially when one considers available fingerprint spoofing techniques.

As a result – and also based on the original survey and consultation with border authorities' representatives – the project enhances its biometric recognition with a palm vein scanner in order to counter spoofing attempts and improve the overall security level. The scanner will perform liveness detection through the illumination of blood vessels via a near infrared light source. What's more, the implementation of the scanner will not hinder the overall transaction time, which in the case of palm vein recognition is calculated to be one second.



Silent Talker: this technology offers an artificial intelligence lie detector that spots tiny changes in facial expressions. Image credit: *Manchester Metropolitan University*

"A deception detection system will analyse a traveller's facial biometrics or micro-expressions as they react to a random question about their travel, to determine whether the person is lying"

One other novel feature developed within the project, which will be tested in real-life scenarios, is an automatic deception detection system. This component of the platform is dedicated to analysing the non-verbal behaviour of travellers. It will be able to provide border officers with an estimated level of deception, based on a video recorded during an interview session at the pre-arrival registration phase.

The tool's architecture is based on the system known as Silent Talker[6]. However, it will be re-engineered in order to perform a broader set of functions. Deployed in pre-arrival interviews, it will conduct an observational analysis of a particular individual and generate a traveller's deception score. An advanced verbal and non-verbal communication border control agent avatar will also boost the system. It will be able to analyse a traveller's facial biometrics (micro-expressions) as the interviewee reacts to a randomly asked question about their travel, in order to determine whether the person is lying.

In summary, controlling borders between different European countries requires maximum-level security, combined with low operational costs and high-speed checks and procedures. Biometric technologies offer a potential solution to deliver high security levels while minimising the impact on travellers' transit time. The proposed Intelligent Portable Control System aims to achieve this, enabling faster and more thorough border control for third-country nationals crossing the land borders of EU member states. To do this, it incorporates software and hardware technologies in a two-stage procedure. This includes fingerprint, palm vein reader and face recognition biometric technology built into a user-friendly portable device which will scan and analyse the biometric information of travellers in a fast, easy and secure way.

Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700626. On behalf of the consortium, the authors would like to express their gratitude to the border guard managers and officers who voluntarily participated in the interviews and offered their constructive answers based on their expertise during the course of this research.

About the authors

Dr Keeley Crockett is a reader in computational intelligence at Manchester Metropolitan University and leader of the Intelligent Systems Group. She has over 20 years' experience of R&D in computational intelligence algorithms and applications including Silent Talker. She is the current Chair of IEEE Women in Engineering UKI. She is co-leading the development of the Automatic Deception Detection System as part of the pre-traveller registration system.

Dr of Law Székely Zoltán is a senior officer in the Hungarian National Police and assistant

lecturer at the National University of Public Service. With 13 years' front-line experience in border control, he is now dealing with national and international security R&D projects. His main focus is on data protection, privacy and use of robots for law enforcement purposes.

Dr James O'Shea is a senior lecturer in computer science at Manchester Metropolitan University. He has relevant expertise in both adaptive psychological profiling and conversational agents. He was a key member of the team that developed Silent Talker, and is a named inventor on the patent relating to the system. He is co-leading the development of the Automatic Deception Detection System.

Łukasz Szklarski is a head of the sensor technology & biometrics department at ITTI Sp. z o.o with a Master's degree in the field of IT. He is a project manager with technical expertise in sensor technologies for surveillance and biometric identification, IT systems, decision support systems, modern security and military technologies. He has participated in a number of projects for the European Commission (eg, TALOS, DESTRIERO, SECTOR, FASTPASS, PROTECT) and the European Defence Agency (eg, CARDINAL, SIMS, UGELAS, CENSIT).

Anna Malamou is an electrical and computer science engineer and holds an MSc in nanotechnology. She is currently finishing her PhD in SAR imaging mathematical and electromagnetic methods. She has worked as an assistant lecturer in universities and colleges (NTUA, ASPETE, AMC). She is the author of several journal papers and co-author of two books. She joined European Dynamics in 2016 as an R&D consultant.

Dr Georgios Boultadakis holds a PhD in radar imaging and signal processing, and a Dipl-Ing degree in avionics systems engineering. He joined European Dynamics in 2014 as a senior R&D consultant. He has worked as an engineering manager for the Hellenic Air Force. He is a research associate of the Radar Systems and Remote Sensing Lab of NTUA. He has participated in several EU research projects and has published a number of scientific papers.

References

1. Balla, J. 'Applying Biometric Data for Personal Identification'. Biztonságpolitika.hu, 1-11 (2013).
2. Varga, J. 'A totális határforgalom-ellenőrzéstől a szelektív és differenciált ellenőrzésig: az 1980-as és 1990-es évek világpolitikai és társadalmi változásai, hatások a határforgalom-ellenőrzésre', 2016. In Deák J; Sallai J; Gaál G. 'A toll sokszor erősebb, mint a kard: rendészettudományi tanulmányok Prof Dr Fórizs Sándor 65. születésnapja tiszteletére'. (old: 267). Budapest: NKE Szolgáltató Nonprofit Kft.
3. Székely, Z. 'Schengen, at the Border and Beyond: Past, present and future', 2014. In N (ed), 'Government vs Governance in Central and Eastern Europe: From Pre-Weberianism to Neo-Weberianism?' (old: 7). Pozsony: NISPAcee.
4. Varga, J. 'Az Integrált Határigazgatás európai uniós rendszere. Hadtudományi Szemle' (2015); 170-176.
5. Fenton, M; Bieman, J. 'Software Metrics: A Rigorous and Practical Approach', Third Edition. Chapman & Hall/CRC Innovations in Software Engineering and Software Development Series, CRC Press, 2014.
6. Rothwell, J; Bandar, Z; O'Shea, J; McLean, D. 'Silent Talker: a new computer-based system for the analysis of facial cues to deception'. Applied Cognitive Psychology, 20(6) (2006); 757-777.

Can cancellable biometrics preserve privacy?

Punithavathi, P

Geetha Subbiah

Punithavathi, P and Geetha Subbiah, VIT University

Biometrics increasingly form the basis of identification and recognition across many sensitive applications. But as the use of biometric systems increases, so do the threats against them. The secure storage of biometric templates has therefore become a key issue in the modern era; the acceptance of biometric authentication devices by the general public is dependent on the perceived level of security of biometric information templates stored within databases.

Privacy concerns have grown because a biometric template is a unique identifier of a person. And while the template cannot be decoded back to the biometric data, it may be used to track the individual. If there is a database that ties the user to their unique biometric template, it could be used illegally to monitor the activities of the user. Such threats need to be addressed, and one potential solution is cancellable biometrics. This is a template transformation technique that uses intentional repeated distortions to provide security to biometric templates; the distortions can be performed either at signal level or at feature level to achieve a transformed template. This article describes the role of a cancellable biometric system.

What is cancellable biometrics?

In essence, a cancellable biometric system (CBS) is a feature/signal-level template transformation approach, where the biometric attribute of a user is altered according to parameters derived from either a user-specific password or key. Only the transformed template is stored in the template database, and matching is performed within the transformed domain. A user can become registered for diverse applications using different templates. The first move toward transformed biometrics was provided by Soutar et al[1] in 1998, but the actual idea of cancellable biometrics was detailed by Ratha et al in 2007[2]. For an illustration of the entire system, see Figure 1.

The CBS is designed to replace the traditional approach in authenticating sensitive applications. But in what way are cancellable biometrics different? Figure 2 shows the